SEMESTER END EXAMINATION APRIL-MAY, 2026

Course Name: - B.Tech **Semester: 8th**

Paper Name: - Cryptography and Network Security **Paper Code: TCS 081**

Time - 3Hrs + 20 minutes per hour extra time for V.I. & examinees with writer. **Max Marks-70**

Instructions:

The question paper consists of three sections namely A, B, C. All sections are compulsory.
Section A- Each question carries **03** marks. All questions are compulsory.
Section B- Answer any **5 out of 7** given questions. Each question carries **7 marks**.
Section C- Answer any **2 out of 3** given questions. Each question carries **10 marks**.

Section – A (खण्ड–अ)

Objective Questions(वस्तुनिष्ठप्रश्न)

1. Answer all the following questions. **5×3=15**

i) Advanced Encryption Standard uses block size of:
a) 64 bits
b) 128 bits
c) 192 bits
d) 256 bits

ii) PGP is used for:
a) Email security
b) Network routing
c) Data compression
d) File transfer

iii) Packet filtering firewall works at:
a) Application layer
b) Transport layer
c) Network layer
d) Physical layer

iv) Which cipher is a substitution cipher?
a) Caesar Cipher
b) Transposition Cipher
c) Playfair Cipher
d) Both a & c

v) Number of rounds in DES algorithm:
a) 8
b) 10
c) 16
d) 32

Section – B

Short Answer Questions

2. Answer any five of the following questions. **5×7=35**

(i) Explain SSL/TLS protocols and their role in secure communication.

(ii) Explain message authentication codes (MAC) and their importance.

(iii) Differentiate between monoalphabetic and polyalphabetic ciphers.

Scanned with OKEN Scanner

(iv) Explain types of malware and their impact on networks.

(v) Describe RSA algorithm in brief.

(vi) Explain RC4 algorithm and its working.

(vii) Compare DES, AES, and RSA in terms of security, performance, and usage.

Section – C
Descriptive Questions

3. Answer any 02 question of the following question. **2×10=20**

(i) Explain firewall design principles and types of firewalls.

(ii) Explain hash functions and message authentication techniques, including their properties and applications.

(iii) Explain the security goals and classify different types of security attacks (Interruption, Interception, Modification, Fabrication) with suitable examples and diagrams.

****

Scanned with OKEN Scanner